Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (14-21), Month: May - August 2023, Available at: www.noveltyjournals.com

MANAGING THE COST OF COMPUTER NETWORK

Seth Okyere-Dankwa[1], Mensah Sitti[2], Anita Antwiwaa[3]

[1]Dean, School of Graduate Stadies, Koforidua Technical University, Kofridua

[2] Lecturer, Computer Science & Eng. Dept. University of Mines & Tech,Tarkwa

[3] Lecturer, Elect,& Eng Dept Cape Coast Technical University, Cape Coast .

DOI: https://doi.org/10.5281/zenodo.7944045

Published Date: 17-May-2023

Abstract: **As networked installations become larger, more complex, and more heterogeneous, the cost of managing it rises. To manage such costs, standardised tools are needed to be employed across a broad spectrum of product types, including end systems, routers, bridges and telecommunications equipment, which can be used in a mixed vendor environment. To meet this demand a simple network management protocol (SNMP) has been developed to provide a tool for multivendor and interoperable network management. This Study reviews two network management protocols and their applicability within a managed network environment. It is inferred from the study that RMON has a lot of advantages over SNMP in the areas of efficiency, remote monitoring and management of large computer network.**

Keywords: **MDB, MIB, NMS, RMON, SGMP SNMP.**

1. INTRODUCTION

Objects of network consist of network elements such as routers, bridges, hubs and so on. These objects can be grouped into managed and unmanaged elements. The managed elements have management process called an agent running on them. The unmanaged elements do not have such facilities. There is a communication between the manager and the agent in the managed element. The manager manages the managed element. The manager has a Management Database (MDB) but the agent does not have. Both the manager and the agent have Management Information Base (MIB) which they use to store and exchange management information. The MDB is a real database and contains administrative or measured configured value of the network elements. The MIB on the other hand is a virtual database and contains necessary information for processes to exchange information. The manager queries the agent and receives management data, process it, and store it in its database. An unsolicited minimal set of alarm message can be sent by the agent to the manager. (Subramanian, 2010).

1.1 Problem Statement

Stallings W. (2013) argued that the starting point for common protocols and standards was the simple gateway monitoring protocol (SGMP) issued in November 1987. SGMP offered a simple means of monitoring gateways. SGMP was picked as baseline and adapted to produce the simple network management protocol when the need for more general purpose network management tool was identified in August, 1988.

SNMP offered a minimal but powerful set of facilities for control and monitoring of network elements employing a simple structure of management information (SMI), management information base (MIB) and protocol. A notable deficiency was the difficulty of networks monitoring, as against the nodes on the networks. Substantial functional enhancement to SNMP was attained by the definition of a set of standardized management objects referred to as the remote network monitoring (RMON) MIB issued in November 1991. RMON indicated a major functional enhancement to the first version of SNMP.

Another inadequacy in SNMP was the total lack of security facilities. A set of documents referred to as a secure SNMP (S-SNMP) was issued in July 1992 as proposed standard to remedy the problem. Simple management protocol (SMP) was

issued outside the Internet standards structure in the same month (July). SMP offered functional enhancements to SNMP and integrated with minor changes, the security enhancements of S-SNMP. It also added some of the concepts from RMON, in addition to the specifications of alarms and events, and the use of a status columnar object to facilitate row creation and deletion. An approval was given for SMP as the baseline for developing a second generation SNMP, known as SNMP version 2 (SNMPv2).

1.2 Objective

The global objective is to minimise the cost of Computer Network operation.

This can be achieved through the following specific objectives.

1. To identify differences between various protocols and their versions
2. To review the Operations of SNMP and RMON
3. To analyse types of Management Information base.
4. To establish appropriateness of a network management protocol in network management system.
5. To design a network management system, use by medium sized enterprise.

2. RELATED WORKS

2.1 Evolution of common protocols and standards

Two working groups were set up to produce SNMPv2. The first working group was charged with non-security aspects, these include protocol, MIB, SMI, conformance statements and coexistence strategies with SNMPv1. The work was largely based on SMP. The group completed it work in 1992 and came out with a set of nine Internet draft documents that were ready to enter the standardisation process as proposed Internet standards.

The second working group, known as the SNMPv2 security working group, went on at a slower pace to develop the security aspects of SNMPv2. The work was largely based on S-SNMP, as revised for SMP. The group produced Internet draft documents which represented broad agreement but with unresolved issues in January 1993. SNMPv2 was revised and reissued in 1996 without security features, because of lack of consensus on what should constitute SNMP security.

To resolve the security problem, a number of independent groups commenced work on security enhancement to SNMPv2. Two competing approaches emerged as front runners, SNMPv2u and SNMPv2* which eventually served as an input to a new IETF SNMPv3 working group, which was contracted in March 1997. This group produced a set of Proposed Internet standards published as RFCs 2271 – 2275 by January 1998.

This document set outlines a framework for adding security features into an overall capability that includes either SNMPv1 or SNMPv2 functionality. The documents also define a specific set of capabilities for network security and access control. The RFCs 2271 through 2275, produced by the SNMPv3 working group, describe an overall architecture plus specific message structures and security features, but do not define a new SNMP PDU format. Thus, existing SNMPv1 or SNMPv2 PDU format must be used within the new architecture. SNMPv3 consists of the security and architectural features defined in RFCs 2271 through 2275 plus the PDU format and functionality defined in the SNMPv2 documents.

3. METHODOLOGY

The study adopted Mixed method. Under this strategy, more emphasis was placed on Descriptive approach. Descriptive research is defined as an attempt to explore and explain while providing additional information about a topic (Shield and Rangarjan, 2013).

3.1 Differences between various protocols/ versions of protocols

3.2.1 RMON 1

The greater part of the RMON specification is devoted to a definition of RMON MIB. The RMON MIB is integrated into MIB II with subtree identifier of 16. This consists of statistics, history, alarm, host, hostTopN, matrix, filter, capture, event and tokenRing groups. The specification of the RMON MIB has the effect of defining a set of functions for remote monitoring.

3.2.2 RMON 2

RMON2 extends original RMON MIB by adding a number of new groups. The groups are protocolDir, protocolDist, addressMap, nlHost, nlMatrix, alHost, alMatrix, usrHistory, probeConfig. The extension gives RMON MIB the capability to monitor protocols above MAC level.

3.2.3 SNMPv2.

Subramanian (2010) argue out clearlythat the major changes in SNMPv2. In spite of the lack of security enhancements, major improvements to the architecture have been made in SNMPv2.

Bulk Data Transfer Message: Two important messages were added. The first being the ability to request and receive bulk data using the get bulk message. This process speeds up the get next request action and is useful for retrieval of data from tables.

The second one is the Manager to Manager Message which deals with interoperability of two network management systems. Communication of management messages is extended between management systems, thus making network management systems interoperable.

The Structure of Management Information (SMI) in SNMPv1 is defined as STD 16, which is described in RFCs 1155 and 1212, along with RFC 1215, which describes traps. They have been consolidated and rewritten in RFCs, 1902 through 1904 for SMI in SNMPv2. RFC 1902 deals with SMIv2, RFC 1903 with textual conventions and RFC 1904 with conformances.

The table enhancements defined columnar object with a Syntax clause, RowStatus, conceptual rows can be added to or deleted from an aggregate object table. A table can also be expanded by augmenting another table to it. This is useful in integrating columnar objects to an existing one.

MIB Enhancement brought about significant changes to the systems and groups of version 1. Internet node in the MIB has two new subgroups that are security and snmpV2. System group changes are under mib-2 node in the MIB. The SNMP entities in version 2 are hybrid, with some of the entries from the SNMP group, and the rest from the groups under the newly created snmpV2 node.

Under transport mapping, several changes to the communication model were made in SNMPv2. Even though UDP is the preferred transport protocol mechanism for SNMP management, other transport protocols can be used with SNMPv2. The mappings required to define other protocols on to UDP are the subject of RFC 1906.

Under textual convention, the decision was to maintain the existing defined class types and apply restrictions to them.

Conformance Statements define a minimum set of compliance capabilities that vendors can offer additional capabilities as options.

3.2.4 SNMPv3.

Two security related capabilities were defined in SNMPv3. They are user based security model (USM) and view based access control model (VACM).

USM offers authentication and privacy (encryption) functions and works at the message level. VACM on the other hand decides whether a given principal is permitted access to particular MIB objects to perform particular functions and it works at the PDU level. (Stallings, 2013)

4. OPERATIONS OF SNMP AND RMON

4.1 SNMP

There are three key components in SNMP managed network. They are network – management systems (NMSs), agents and managed devices. The managed device is a network node with an SNMP agent and which resides on a managed network. The managed device collects and store management information and use SNMP to make the information available to NMSs. Managed devices can be hub, switch, router, printer, access server or computer host. An agent in a network is a network management software module that resides in managed device. An agent has local knowledge of management information and translates the information into a form compatible with SNMP. NMS executes applications that monitor and control managed

devices. At the moment, three versions of SNMP are defined: SNMP v1 , SNMP v2 and SNMP v3 . The table4 below offers the summary of the operations and features of the different version of SNMP: (Burke, 2010)

Table 4: Summary of different version of SNMP

SNMP v1	**Basic Operations and Features**
Get	The NMS uses to retrieve the value of one or more object instances from an agent
GetNext	The NMS employs to retrieve the value of the next object instance in a table or a list within an agent
Set	The NMS uses to set the values of object instances within an agent.
GetResponse	The agents use as a respond to the NMS supplying the requested value(s).
Trap	The agents use to asynchronously inform the NMS of a significant event.
SNMP v2	**Additional Operations and Features**
GetBulk	The NMS uses to efficiently retrieve large blocks of data.
Inform	Permits one NMS to send trap information to another NMS and to then receive a response.
SNMP v3	**Security Enhancement**
	User-based Security Model (USM) for SNMP message security.
	View-based Access Control Model (VACM) for access control.
	Dynamically configure the SNMP agents using SNMP SET commands.

Source: (Burk, 2010)

4.2 RMON

Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs.

Two versions of RMON are defined: RMON1 (RMONv1) and RMON2 (RMONv2). RMON1 defined ten MIB groups for basic network monitoring, which can now be found on most modern network hardware. RMON2 (RMONv2) is an extension of RMON that focuses on higher layers of traffic above the data link layer (layer 2). RMON2 has an emphasis on IP traffic and application-level traffic. RMON2 allows network management applications to monitor packets on all network layers. This is different from RMON1 which only allows network monitoring at data link layer or below.

RMON comprises of two components: a probe (or an agent or a monitor), and a client, usually a management station. Agents store network information within their RMON MIB and are normally found as embedded software on network hardware such as routers and switches although they can be a program running on a PC. Agents can only see the traffic that flows through them so they must be placed on each LAN segment or WAN link that is to be monitored. Clients, or management stations, communicate with the RMON agent or probe, using SNMP to obtain and correlate RMON data. Now, there are a number of variations to the RMON MIB. For example, the Token Ring RMON MIB provides objects specific to managing Token Ring networks. The SMON MIB extends RMON by providing RMON analysis for switched networks.

4.3 Types of Management Information.

4.3.1 SNMP

The management information base (MIB) has a hierarchical tree structure. Each object within the MIB has an object identifier which defines its position in the tree. Each object has a name. Groups of objects which are related are also defined. Each object has a type such as “integer”. Types can be simple or constructed. Object with simple type has one value whereas an object with constructed type contains other objects that are of simple type, but may not be the same simple type. ASN.1 specifies object types defined and the format for definition. The format contains, name of object, its type, whether it is accessible by a Management Station, if so, whether it is read only, read write or not accessible and a brief text description of

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (14-21), Month: May - August 2023, Available at: www.noveltyjournals.com

the object. RFC 1155 described the language use to define MIB. The structure of management information (SMI) is a specification of how information is to be managed on TCP/IP networks. Some of the objects in the SMI object tree, starting from the tree root, are shown in fig.4 below. The present MIB standard is MIB-2. It contains ten groups with the names: system, interfaces, address translation (at), internet protocol (ip), internet control management protocol (icmp), transmission control protocol (tcp), unreliable datagram protocol (udp), exterior gateway protocol (egp) transmission, and simple network management protocol (snmp). Most vendors have created proprietary MIBs for their devices. Those MIBs are listed under the enterprise node which is a sub node of private (4) in fig.4 below. (Burke, 2010).

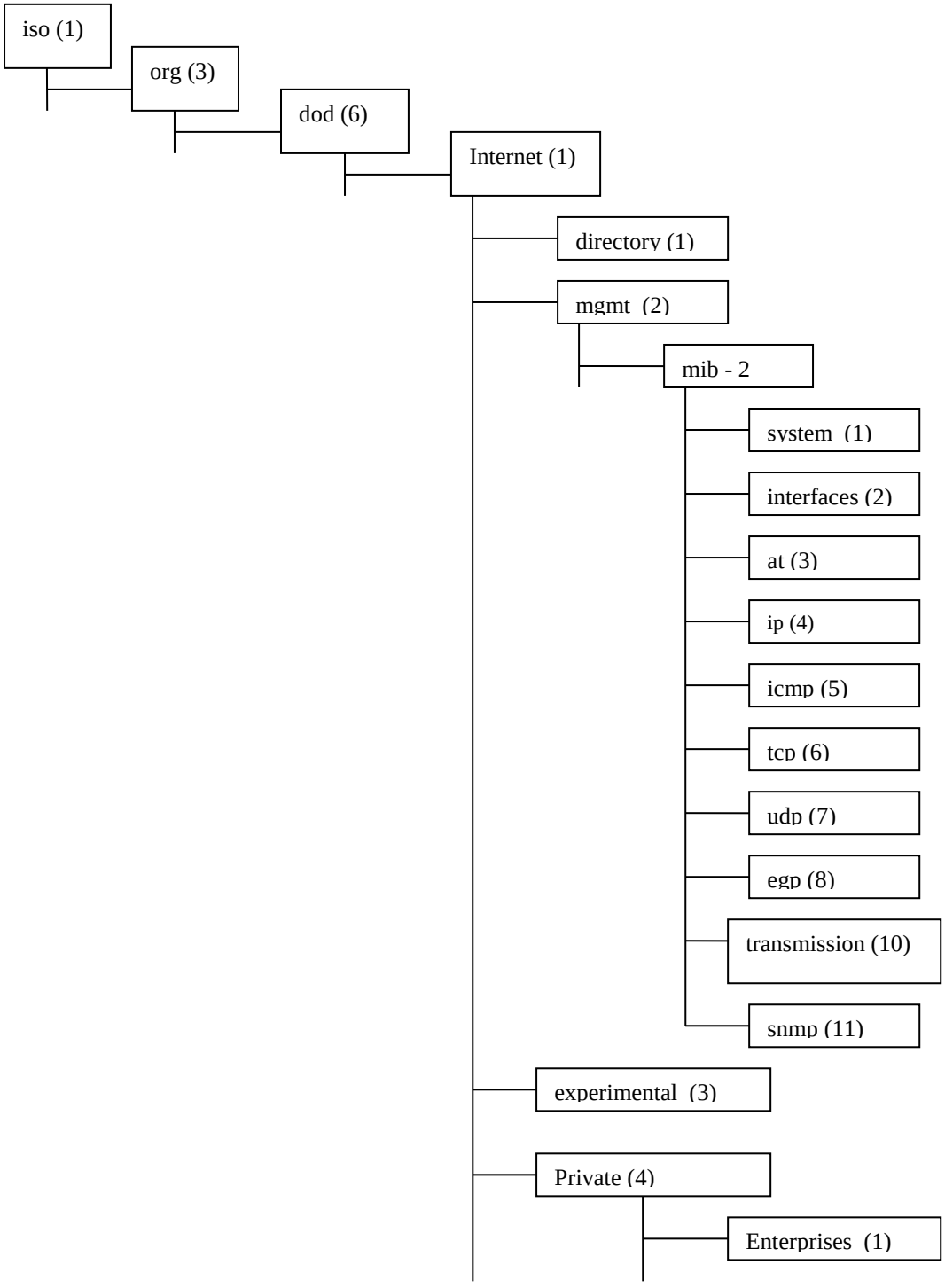


Fig 4: MIBs listed under the enterprise node. Source (Burke, 2010).

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (14-21), Month: May - August 2023, Available at: www.noveltyjournals.com

4.3.2 RMON

The RMON MIB is incorporated into MIB-II with a sub tree identifier of 16. They are divided into ten groups which are:

- statistics
- history
- alarm
- host
- hostTopN
- matrix
- filter
- capture
- event
- tokenRing

Each group is used for data storage and statistics obtained from data collected by the monitor. The stored data in each group represent data gathered from one or more attached subnetworks, this depend on the configuration of the monitor used for that particular group.

Apart from alarm which requires event group to be implemented, hostTopN which requires implementation of host group and packet capture group which requires filter group to be implemented. All the RMON MIB groups are optional. Groups like tokenRing, matrix, hostTopN, host, history and statistics are primary concerned with collection of traffic statistics for one or more subnetworks. Groups like event, capture, filter and alarm are concerned with various alarm conditions and with filtering of packets based on user-defined criteria.

RMON2 MIB is an extension of RMON MIB with a number of new groups. The groups are :

- protocolDir
- protocolDist
- addressMap
- nlHost
- nlMatrix
- alHost
- alMatrix
- usrHistory
- probeConfig

RMON2 introduces two new features not found in RMON1 that enhance the power and flexibility of RMON. They are both in the area of table indexing and are indexing with external objects and time filter indexing. The definition of use of index clause in object type macros in SNMPv1 is not clear whether an index object is required to be a columnar object in the table that it indexes. RMON2 uses indexing with external objects to tie together control tables and data tables. Time filter indexing is an efficient mechanism used by RMON2 to poll only values of objects which have changed at the probe since the last poll instead of polling the whole values. There is no direct way in SNMPv1 or SNMPv2 to achieve this function. RMON2 matrix groups gather statistics based on network layer address and on application level protocol. The probe configuration group is designed to enhance interoperability among RMON probes and managers by defining a standard set of configuration parameters for probes.

4.4 Compare and contrast SNMP with RMON

- SNMP is not suitable for the management of large network because of performance limitations of pulling. RMON on the other hand is suitable for large network because of it ability to monitor local network segment and does the necessary analysis.
- RMON pings locally thus having the possibility of losing fewer packets as compare to SNMP which does not ping locally.

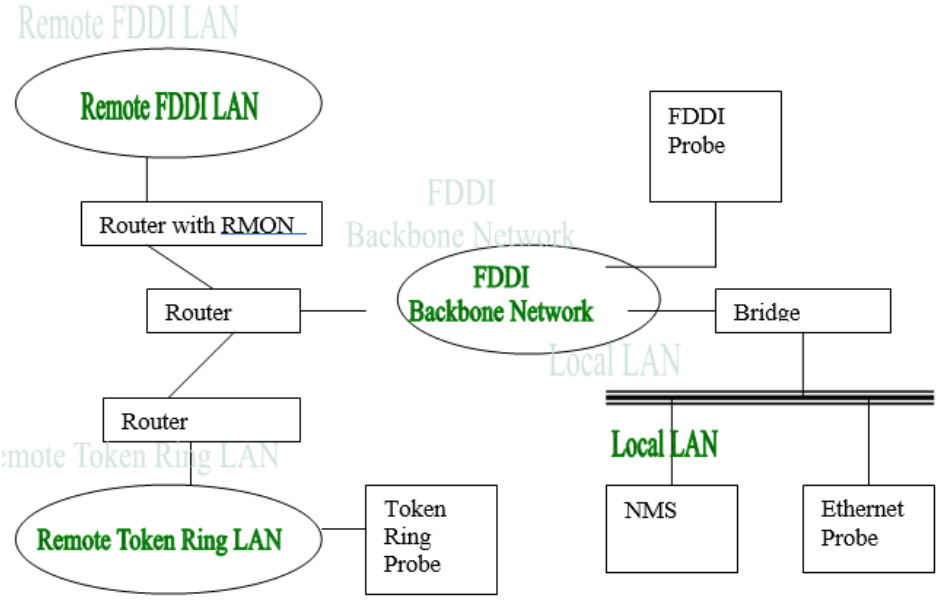
- RMON ensures higher network availability than SNMP because its operation reduces congestion.
- RMON (RMON2) is able to monitor packets at layers 3 through 7 of the OSI model whilst SNMP is limited to layer 2.
- RMON device monitors local segment of the network whilst SNMP device monitors individual devices like switches, hubs, routers etc.
- RMON uses efficient mechanism call Time filter indexing to poll only values of objects which have changed at the probe since the last poll instead of polling the whole values. There is no direct way in SNMPv1 or SNMPv2 to achieve this function.
- SNMP is simple to implement, thus many vendors have it on their devices. RMON on the other hand need to be installed on each LAN segment to ensure remote monitoring.
- Even though RMON operation is effective and efficient, initial invest cost is far high than SNMP.

4.5 Appropriateness of a network management protocol in network management system.

RMON is more appropriate than SNMP in a network management system which has been configured as a three tier. In this case, one of the layers serves as both agent and manager. Such layer could be employed at local site of the network to monitor, gather and analyse information locally and then transmit to a remote network management station. RMON devices play such role as mentioned in section 4.2, thus making RMON suitable for management of large network system. RMON technology is also appropriate for offering network availability for users and greater productivity for network administrators.

4.6 Design of network management system use by medium sized enterprise.

The diagram (figure 4.1) below shows the design of a network management system recommended for use by a medium sized enterprise. The diagram depicts FDDI backbone with a local Ethernet LAN. The backbone network is connected to by two remote LANs namely FDDI LAN and token ring LAN. The network management system is contained in the Local LAN. The token ring LAN is monitored by the token ring probe and the probe communicates to the NMS through the routers. The Remote FDDI LAN is monitored by the router with RMON. The FDDI probe communicates with the NMS. The four probes which monitor the four LANs and communicate with the NMS are RMON devices. The advantages of using these devices are stated in section 4.2 of the study. As stated in section 4.2, because RMON can decode packets at layer 3 and above at OSI model, RMON probe is able to monitor traffic on the basis of network-layer protocols and addresses, including the Internet Protocol (IP). By doing this, the probe is able to monitor beyond the LAN segment to which it is attached and view inbound traffic onto the LAN via routers. The RMON probe also base on its ability to decode and monitor application- level traffic, can record traffic to and from hosts for particular applications. (Subramanian, 2010).



Source: (Okyere-Dankwa et al 2023)

Figure 4.1: Design of a network management system recommended for use by a medium sized enterprise

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (14-21), Month: May - August 2023, Available at: www.noveltyjournals.com

5. CONCLUSION

The study has examined a network management system. The study has also outline the metamorphosis of both SNMP and RMON, compare and contrast their performance. It is inferred from the study that RMON has a lot of advantages over SNMP in the areas of efficiency, remote monitoring and management of large computer network.

REFERENCES

[1] Burke, J. R. (2010) Network Management. Concepts and Practice: A Hand –on Approach. New Jersey: Prentice Hall.

[2] Feldmier, J. (2018) Network Traffic Management. Unix Review

[3] Leinwand, A. and Conroy K. F. (2007) Network Management. A Practical Perspective. Second Edition. New York: Addison- Wesley.

[4] Mikalsen, A. and Borgesen, P. (2002) Local Area Network Management, Design and Security. A Practical Approach. New York: John Wiley.

[5] Mauro, D. and Schmidt, K. (2018) Essential SNMP. California: O' Reilly.

[6] Oetiker, T. and Rand, D. (2020) Multi Router Traffic Grapher. http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html

[7] Okyere-Dankwa S., Mensah Sitti and Antwiwaa A. (2023) Managing the cost of computer network.

[8] Oliver, N. and Oliver, V. (2006) Computer Networks Principles, Technologies, and Protocols for Network Design. West Sussex: John Wiley.

[9] Shields, P. and Rangarjan, N. (2013). A Playbook for Research Methods: Integrating Conceptual Frameworks and Project Management. Stillwater, OK: New Forums Press

[10] Subramanian, M. (2010) Network Management Principles and Practice. New York: Addison-Wesley.

[11] Stallings, W. (2013) SNMP, SNMPv2, SNMPv3 and RMON1 and RMON2.Third Edition. New York : Addison – Wesley Professional.

[12] Tanenbaum, A. S. (2010) Computer Networks. Fifth Edition. New Jersey: Prentice Hall PTR.